RECOMENDACIONES DIRIGIDAS A PADRES, TUTORES Y DOCENTES PARA LA CIBERSEGURIDAD DE NIÑOS, NIÑAS, ADOLESCENTES Y JÓVENES

Mantener **la ciberseguridad de la comunidad educativa requiere de la participación activa de los padres, tutores, docentes y autoridades escolares para que puedan ayudar a los estudiantes** a hacer un uso de las redes y dispositivos de telecomunicaciones de manera segura, responsable y positiva, reconociendo que niños, niñas, adolescentes y jóvenes deben contar con todas las herramientas y el conocimiento para manejar su vida *online* con seguridad, poniendo a su disposición los recursos para que puedan acceder a ayuda y apoyo especializado.

A continuación se presentan algunas recomendaciones de ciberseguridad dirigidas a padres, tutores y docentes:

- Es necesario conocer sobre las amenazas y riesgos a los que se enfrentan niños, niñas, adolescentes y jóvenes al utilizar dispositivos, plataformas, aplicaciones, comunicaciones y tecnologías de la información, y de igual forma se deben conocer las acciones para prevenir y enfrentar dichos riesgos, así como para controlar los daños en caso de incidentes de ciberseguridad que afecten integridad y bienestar físico y emocional.

- Es muy importante conversar con niños, niñas, adolescentes y jóvenes sobre los temas de acoso y el peligro que representa compartir información y entablar cualquier tipo de comunicación con extraños.

- Se debe mantener un diálogo constante y abierto con niños, niñas, adolescentes y jóvenes para promover una cultura de ciberseguridad, creando una red de apoyo para que se sientan cómodos buscando ayuda. Es fundamental mantenerse atento a cualquier signo de angustia.

- Es importante verificar con regularidad el uso que niños, niñas, adolescentes y jóvenes dan a la tecnología que tienen a su disposición, se debe estar familiarizados con los sitios que visitan regularmente, identificar qué tipo de actividades realizan en línea, el contenido que comparten, cómo están utilizando teléfonos celulares, tabletas, computadoras, así como qué nuevas herramientas y aplicaciones podrían estar usando.

- Es primordial fomentar el pensamiento crítico en niños, niñas, adolescentes y jóvenes para que analicen el tipo de información a la que tienen acceso. El análisis y la discusión de ciertos contenidos en línea ayudará a que se formen un criterio para la identificación de contenido regular, publicidad engañosa y contenido falso o dañino que promueva la desinformación, la violencia, la discriminación y las conductas de riesgo.

- Siempre que sea posible, es fundamental establecer reglas para administrar el tiempo frente a la pantalla, así como los límites para las actividades en línea. Es necesario promover un equilibrio entre el tiempo en línea y otras actividades.

- Se debe fortalecer las capacidades de niños, niñas, adolescentes y jóvenes para superar los desafíos que se presentan en el mundo digital, los cuales pueden generar angustia, ansiedad, enojo, tristeza, aislamiento, etcétera, para esto hay que poner en práctica algunas estrategias que ayuden a identificar las situaciones adversas y a enfrentarlas de manera positiva.

ATENTAMENTE
DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

RECOMENDACIONES DE CIBERSEGURIDAD PARA NIÑOS, NIÑAS, ADOLESCENTES Y JÓVENES EN LÍNEA

Lo que SÍ se debe hacer

- Identificar e informar a padres, tutores o docentes sobre contenido potencialmente dañino o ilegal, así como sobre cualquier amenaza o situación negativa en las redes sociales o plataformas que se utilizan.
- Usar un alias o nombre alternativo como nombre de usuario para interactuar con otros en línea.
- Aplicar la configuración de privacidad a las cuentas de redes sociales, de modo que las publicaciones solo sean visibles para amigos cercanos y conocidos.
- Reportar en sitios web o redes sociales cualquier situación abusiva, ofensiva, amenazante o comportamientos inapropiados.
- Informar inmediatamente al administrador de los servicios si se sospecha que alguna cuenta (por ejemplo de correo electrónico o redes sociales) ha sido hackeada.
- Compartir número de teléfono únicamente con familiares y amigos cercanos.

Lo que NO se debe hacer

- **NO** compartir información personal (nombre completo, fecha de nacimiento, número de teléfono, etcétera) de uno mismo o de sus familiares si no es necesario. Proteger con contraseña los dispositivos donde se almacene información personal.
- **NO** publicar en redes todas las actividades cotidianas.
- **NO** enviar fotos a personas desconocidas, especialmente si éstas son con poca o nula ropa, tampoco se deben compartir este tipo de imágenes en redes sociales.
- **NO** responder a mensajes de personas que no se conozcan. Nunca abrir correos electrónicos ni archivos adjuntos de remitentes desconocidos.
- **NO** compartir contraseñas con terceros por ningún medio (papel, mensaje de texto, *inbox* o correo electrónico), de igual forma no se deben ingresar contraseñas en presencia de otras personas.
- **NO** utilizar ni difundir en medios electrónicos información de otras personas sin su consentimiento.
- **NO** organizar ni acceder a encuentros con desconocidos, si algún extraño lo solicita se debe informar inmediatamente de la situación a un adulto o persona de confianza.

ATENTAMENTE

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

EDUCACIÓN

SECRETARÍA DE EDUCACIÓN PÚBLICA